2021 NERC Critical Infrastructure Protection Security Awareness Training
Applicability

- All WAPA Federal and Contract employees are required to complete annual North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) security awareness training
## Contents: CIP Security Awareness Training (CIPSAT)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>NERC Critical Infrastructure Protection training introduction</td>
<td>4-7</td>
</tr>
<tr>
<td>Key Terms</td>
<td>8-9</td>
</tr>
<tr>
<td>Cyber Security Policies</td>
<td>10</td>
</tr>
<tr>
<td>Physical Access Controls</td>
<td>11-13</td>
</tr>
<tr>
<td>Electronic Access Controls</td>
<td>14</td>
</tr>
<tr>
<td>Visitor Control Program</td>
<td>15-16</td>
</tr>
<tr>
<td>Handling of BES Information and Its Storage</td>
<td>17-18</td>
</tr>
<tr>
<td>Incident identification and notification</td>
<td>19</td>
</tr>
<tr>
<td>Recovery Plans</td>
<td>20</td>
</tr>
<tr>
<td>Response to Cyber Security Incidents</td>
<td>21</td>
</tr>
<tr>
<td>Risks associated with interconnectivity</td>
<td>22-23</td>
</tr>
<tr>
<td>Information Protection and BCSI</td>
<td>24-26</td>
</tr>
<tr>
<td>Change Control and Configuration Management</td>
<td>27-28</td>
</tr>
<tr>
<td>Transient Cyber Assets and Removable Media</td>
<td>29-30</td>
</tr>
<tr>
<td>Additional Training</td>
<td>31</td>
</tr>
<tr>
<td>Addendum: Resources and Links</td>
<td>32</td>
</tr>
</tbody>
</table>
NERC CIP training requirements

• All WAPA Employees (federal and contractor) must complete annual CIP Security Awareness Training (CIPSAT) which is comprised of these slides.

• WAPA will also provide, at least once each calendar quarter, awareness training that reinforces cyber security practices for WAPA personnel who have authorized electronic/logical or authorized unescorted physical access to Bulk Electric System (BES) Cyber Systems. This quarterly awareness training may consist of WAPA publications, email, posters, and presentations.
NERC CIP training requirements (cont.)

Included in this CIP Security Awareness Training are the following topics:

1. Cyber security policies
2. Physical access controls
3. Electronic access controls
4. The visitor control program
5. Handling of BES Cyber System Information and its storage
6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan
7. Recovery plans for BES Cyber Systems
8. Response to Cyber Security Incidents
9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.
NERC CIP training requirements (cont.)

Completion of CIP Security Awareness Training (CIPSAT) is required prior to granting authorized electronic/logical access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.

This training is also required for informational access, unless handling requirements are covered by other legal means (such as a non-disclosure agreement).
Additional training goals

Ensure employees:

• Understand physical and electronic/logical access controls to prevent NERC violations and protect BES Cyber Assets

• Properly handle and control information

• Develop awareness of the “rules of behavior” unique to accessing, operating, changing, and maintaining BES Cyber Assets
Key terms

The following terms may be referenced in this training and are important to understand for general CIP Security Awareness.

- **Bulk Electric System (BES):** As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.

- **BES Cyber System:** One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

- **BES Cyber Assets:** A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

More information and additional terms may be referenced on the NERC web site. A link is provided in the Addendum: Resources and Links, located at the end of this training.
Key terms (cont.)

- **Critical Assets**: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

- **Cyber Assets**: Programmable electronic devices and communication networks including hardware, software, and data.

- **Transient Cyber Assets**: A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP containing high or medium impact BES cyber systems, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

- **Protected Cyber Asset** (PCA)

- **Physical Access Control System** (PACS)

- **Electronic Access Control and Monitoring** (EACM)
CIP Security Awareness Training Content:

1) Cyber security policies
Federal and contract employees with authorized logical access and/or authorized unescorted physical access to a BES Facility or BES Cyber Asset must be familiar with:

- WAPA Rules of Behavior
- WAPA Policy 205.2F Cyber Security and Security Management
- WAPA Order 470.1I Safeguards and Security Program
- WAPA Order 471.3A Information Control
2) Physical access controls

Physical CIP Access:

1. All BES Cyber Systems are contained within a Physical Security Perimeter (PSP).
2. Only personnel with current authorization may enter the PSP without an escort. Never loan/share your badge or key with another individual. Report a lost or stolen badge or key immediately.
3. Tailgating (following, or allowing someone to follow) is prohibited, as NERC CIP requires that each individual be logged when passing through a PSP.
4. Authorized physical access to a PSP is controlled and monitored by means of an electronic Physical Access Control System (PACS). The PAC will grant access at medium impact facilities using a badge only. Access at a high impact facility will require both a badge and PIN.
5. The PACS or a lock will grant access at low impact facilities. (refer to next slide)
CIP Security Awareness Training Content:

Physical access controls (cont.)

Physical Security is afforded to all WAPA Low Impact BES Cyber Systems and physical access is based on need. At a minimum, the physical security afforded shall include at least one of the following, as deemed most appropriate by WAPA:

- The BES Cyber System is located within a locked building when not attended.
- The BES Cyber System is located within a building with entrances which are alarmed through a PACS system.
- The BES Cyber System is located within a building with entrances which are alarmed through a SCADA system.
- The BES Cyber System is located within a locked cabinet.
Physical access controls (cont.)

Physical CIP Access – Any Facility:

• In the event of a badge failure the individual requiring access must contact the Security Operations Center (SOC) with their name and assigned PACS PIN. The on-duty Officer will confirm access is authorized in the PACS, and verify the name/PACS PIN combination is correct before granting access remotely over the PACS. Personnel shall contact the on-duty Officer when departing.

• In the event of a PACS system failure, a mechanical key-override process is instituted. Individuals requiring access to an override key must contact the SOC and verify identity by stating name and PIN. The on-duty Officer confirms access is authorized in the PACS and verifies that the name/PIN combination is correct before disclosing the key box combination.

• For additional information, contact your regional OSEM representative.
CIP Security Awareness Training Content:

3) Electronic/Logical access controls

Electronic CIP Access:
• NERC CIP Standards require that all logical access be logged when passing through a “Electronic Security Perimeter” when using a user ID and password
• Logical (electronic) access records must be kept at least 90 days.
• Logs must be kept longer if related to a reportable incident.

Unless exempted in writing:
• DO NOT connect an outside digital device (transient cyber asset or removable media) to any asset within the electronic security perimeter. This includes devices such as: USB/thumb drives, CD/DVD, mobile phones, and laptops. Approval for use of these devices must be obtained in writing by the responsible manager and should be assessed for risk by Cyber Security.
• DO NOT download software of any type or add or remove assets unless approved via the CIP Change Management Process.
• DO NOT Use a BES Cyber Asset for personal use. These assets are for business mission use only.

Laptops may connect to the WAPA GSS network for updates to anti-virus, Operating System, Applications, or other approved changes and then connect to CIP Low, Medium and High impact sites.
CIP Security Awareness Training Content:

4) The visitor control program

Visitor Controls - When escorting visitors within a CIP Physical Security Perimeter (PSP) it is your responsibility to:

• Understand that only those people with current authorization to enter the PSP can escort visitors or other unauthorized individuals into the PSP.
• Continually escort any individual who does not have authorized, unescorted access.
• Enter the area before the escorted person and leave the area after the escorted person.
• Maintain continuous line of sight or dedicated focus of the unauthorized person(s)
• Limit the visitors to no more than five per escort and keep in close proximity
• Conduct a proper handoff of escorting duties if you need to depart the area. This handoff must include:
  • Ensuring the new escort has authorized, unescorted privileges within the PSP
  • Briefing the escort on the visitors present, including names, orgs, purpose for entering the PSP, time entered, and how access into the PSP was logged
  • Verbal confirmation from the new escort that they understand they are assuming all escorting responsibilities and understand what those responsibilities entail
  • Notifying the visitors present of who is the new escort
4) The visitor control program (cont.)

Visitor Controls - When escorting visitors it is your responsibility to:

- Know the logging procedures your Region uses and log all visitors into a PSP
- Visitors must either sign the associated CIP area visitor log or call the associated SOC who records visitor information on a Daily Activity Report (DAR).
  - Recorded visitor information includes date and time of the initial entry and last exit, visitor name, and name of responsible host.
  - It is the responsibility of the escort to ensure that visitors complete all fields listed in the visitor log or all visitor information is reported to the SOC.
- Ensure no visitor harms the integrity of the critical cyber assets or interferes with the reliability of the Bulk Electric System.

NOTE: CIP area Visitor Logs and DARs are collected and reviewed quarterly.
5) Handling of BES Cyber System Information (BCSI) and its storage

BCSI Protection:

Users are responsible for protecting BCSI from unauthorized access.

Users will not attempt to access any BCSI or programs contained on any system for which they do not have authorization or explicit consent of the owner of the system.

Before sharing BSCI, verify that those you share with have access authorization to that information.
5) Handling of BES Cyber System Information (BCSI) and its storage (cont.)

Additional practices to follow to protect BCSI:

• Lock the workstation before you leave.
• Encrypt Official Use Only (OUO) and Personally Identifiable Information (PII) for electronic storage and/or transmission.
• Protect media from adverse environmental conditions, such as heat and magnetic fields that can cause damage.
• Handle and process Engineering information as per WAPA O 471.3A (Information Control Order)
• BES Cyber System Information contained on Transient Cyber Assets must be properly managed per WAPA policy and procedures. (Refer to the topics for Transient Cyber Assets, and Information Protection elsewhere in this training)
6) Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan

Be aware of how to identify incidents, as identified in the WAPA Cyber Security Incident Response Plan (CSIRP).

Report suspected cyber security incidents immediately to WITCC or your Information System Security Officer (ISSO).

Incident identification and detection is described in WAPA’s Cyber Security Incident Response Plan (CSIRP):

“An incident is a violation or the threat of a violation of information security policies, acceptable use policies and/or other security policies. Examples of incidents include a Denial of Service (DoS) to a WAPA’s web page, download and installation of malware through email or a web page, WAPA data loss not released through approved agency methods, the disclosure or compromise of WAPA credentials into a web site not managed by WAPA, or an unplanned disruption or the attempt of disruption to the BES by unauthorized personnel through a cyber security control.”

Reference: WAPA Cyber Security Incident Response Plan (CSIRP).
7) Recovery Plans for BES Cyber Systems

• Become familiar with the Recovery Plan for the assets in your area.
• Know the roles you may be assigned for Recovery activity.
• Ensure that Recovery Plans are exercised periodically, at least annually.
• Be familiar with any backup and restore procedures for assets in your area.
• Backup and recovery of assets must be tested periodically, as defined in their recovery plan.
• Identify any lessons learned that are determined from Recovery tests, exercises, or real recovery activities.
• Update recovery plans to reflect lessons learned from recovery tests, exercises, or actual recoveries.
• Notify those with roles in the recovery plan of the update to the plan.
CIP Security Awareness Training Content:

8) Response to Cyber Security Incidents

Reporting Incidents:
Employees will report all incidents or attempts of anyone trying to gain unauthorized access to BES Cyber Assets or other computer resources to the proper authorities by contacting the WAPA IT Call Center (720-962-7111), your Cyber Security Officer, or your IT Manager.

Reference: WAPA Cyber Security Incident Response Plan (CSIRP).
CIP Security Awareness Training Content:

9) Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

Know the risks associated with systems interconnectivity:

• Risks associated with exposing connections outside the boundary, leading to loss of confidentiality, integrity, and availability.

Know the risks associated with transient cyber assets and removable media:

• Risk from exposure to malware.
• Risks associated with loss or theft.
• Risks associated with unencrypted information, leading to loss of confidentiality.
• Risks associated with moving cyber assets such as removable media from a low security enclave to a higher security enclave (and vice versa).
CIP Security Awareness Training Content:

9) Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

(cont.)

Any new BES Cyber System connections must be formally reviewed and approved by Cyber Security personnel and/or managers of those systems via the appropriate Change Control and Configuration Management Processes.

Changes to existing BES Cyber System connections must be formally reviewed and approved by Cyber Security personnel and/or managers of those systems via the appropriate Change Control and Configuration Management Processes.
Information Protection and BCSI

- Information Protection Officers (IPOs) will manage classification and categorization decisions for information – only these IPOs can designate information as BES Cyber System Information, or “BCSI”. The IPOs are members of the IT Cyber Security Information Assurance Group (refer to points of contact on slide 81) and the IT Cybersecurity Compliance Support Group.

- Physical protection of OUO, including BCSI, is required in unmanned facilities, such as substations.

- Follow best practices in your office – lock computer, file or put away paper.

- Encrypt BCSI and other OUO information whenever technically feasible, both data at rest (files) and data in transit (email).

- Mobile device require additional protection. A signed user agreement (currently under development) will be required for personal phones as well as work phones accessing WAPA information including email.

- Become familiar with best practices for media sanitization and destruction of disposed assets containing information as described in WAPA O 471.3A.

- Consult with your Information Cyber Security Officer (ISSO) for additional information.

- Reference WAPA’s Information Control Order WAPA O 471.3A.
BSCI updates
Approved locations and procedures

- Approved Systems designated for storing BCSI:
  - Maximo - Asset Management System
  - Engineering Design Drive – Access Controlled CIP File Storage
  - Cybersecurity Compliance Support SharePoint Site: https://compliance.wapa.int
  - ASPEN Relay Database

- To get access, your supervisor must request your entitlements to these sites using WAYS (where you can filter available roles using “CIP”)
BSCI updates
Approved locations and procedures (cont.)

- Example WAYS BCSI Related Access Entitlements:
  - CIP Aspen
  - CIP Maximo
  - CIP SharePoint <insert specific library names>
  - CIP Engineering Drawings <insert region>
- WAYS requires your supervisor to include a statement of your need for access with the request.
- Access authorization should be verified before sharing BCSI.
Change Control and Configuration Management

• Additions or Changes to BES Cyber Systems must go through the Configuration Change Management Process
• The Change Control Process includes cyber security testing and baseline management
• The Change Control Process will require that a baseline be performed on all assets. This will include all High (i.e. Control centers) and Medium (i.e. Substations) Impact Bulk Electric System (BES)
• Baseline elements required by Change Control Process are as follows:
  • Operating System or firmware of BES asset
  • Commercial or open source application software installed on BES asset
  • Custom software installed on BES asset
  • Logical network port accessible on BES asset
  • Security patches applied on BES asset
Change Control and Configuration Management (cont.)

• The Change Control and Configuration Management Process will utilize Service Now (WAYS) for its workflow and tracking.
• Prior to implementing any change in the production environment (additions, removals or changes), testing will need to be preformed and documentation of the results will be maintained through the Change Control and Confirmation Management process.
• Any changes that affect the baseline elements will need to be processed through Change Control. For a change that deviates from the existing baseline configuration, the baseline configuration will need to be updated within 30 calendar days of completing the change.
• Every High Impact BES asset’s baseline will be monitored at least once every 35 calendar days for changes.
Transient Cyber Assets

Per the NERC Glossary, a Transient Cyber Asset is defined as: A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

In plain English terms, transient cyber assets includes such things as USB sticks, portable hard drives, CD/DVD media, or devices such as laptops and mobile phones. These devices have the capability to store and transfer files from one area to another, and thereby pose risks that must be mitigated.
Transient Cyber Assets (cont.)

Transient Cyber Assets (otherwise known as mobile devices/mobile media) pose a risk to the BES environment if not properly managed.

Be aware that transient cyber assets have requirements for:

• Device authorization
• Software authorization
• Security patch management
• Malware prevention
• Unauthorized use
• Contact your cyber security officer and your supervisor for more information on procedures and best practice.
Additional Training

• In addition to the CIP Security Awareness Training (CIPSAT), additional training may be required based upon your position, role, job duties, and access to WAPA information, assets, or external (non-WAPA) facilities.
• Discuss with your supervisor any additional training that may be required for your position, job duties, and access.
• Training may be required for non-WAPA personnel who need to access WAPA facilities.
Addendum: Resources and Links

- NERC CIP Standards: [http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx](http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx)